基于 Renyi 熵的 Openflow 信道链路泛洪攻击主动防御方法 *

蔡佳晔，张红旗，宋佳良

(信息工程大学，郑州 450001)

摘 要：针对新型链路泛洪攻击，提出一种基于 Renyi 熵的 Openflow 信道链路泛洪攻击主动防御方法。运用 Renyi 熵分析攻击者在构建 Openflow 信道 Linkmap 过程中产生的 ICMP 超时报文数量变化。一旦出现攻击前兆由流量监控服务器向控制器发出攻击预警，控制器启动交换机-控制器连接迁移机制，将交换机迁移至新的控制器下并使用新的 Openflow 信道与之通信。实验证明，主动防御方法能有效避免控制器与交换机之间通信链路受到链路泛洪攻击的影响，确保控制器和交换机能持续交互提供网络服务，增强了 SDN 网络的健壮性。

关键词：链路泛洪攻击；Openflow 信道；Renyi 熵；主动防御

中图分类号：TP393　　doi: xxxxxx

Active defense method of Openflow channel link flooding attack based on Renyi entropy

Cai Jiaye, Zhang Hongqi Song Jialiang

(*Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: For defending the new link flooding attack, this paper proposed an active defense method of Openflow channel link flooding based on Renyi entropy. Analyzing the changes in the number of ICMP timeout messages produced by an attacker in the construction of the Openflow channel Linkmap from Renyi entropy. Once attacks precursor was detected, flow monitoring server sends an attack warning to the controller, then controller start switch-controller connection migration mechanism, migrate the switch to a new controller and communicate with the new Openflow channel. Experimental results show that the active defense method can effectively avoid the impact of link flooding attack between controller and switch and ensure that controller and switch can provide continuous network services and enhance the robustness of SDN network.

Key words: link-flooding attack; Openflow channel; Renyi entropy; active defense

0　引 言

近年来，一种名为链路泛洪攻击(link-flooding attack，LFA)的新型 DDoS 攻击引起学术界的广泛关注。不同于传统 DDoS 攻击以消耗目标服务器资源为目的，链路泛洪攻击旨在泛洪特定网络链路，阻止用户访问某个重要网络服务，间接破坏依赖这些链路的网络服务。链路泛洪攻击的实施策略相比普通 DDoS 攻击更加复杂，隐蔽性更高，其使用合法流量对目标链路实施攻击，使得网络防御机制无法进行有效应对。目前主流的链路泛洪攻击分为 crossfire[1]和 coremelt[2]，其中 crossfire 因其不依赖于 bots 所处位置信息，所以在攻击发起前可以灵活指定不同的链路集合以达到避免引起警报的目的，相比于 coremelt 攻击更具威胁性。

攻击者发动链路泛洪攻击前需要收集目标服务器周围的链路信息，通常攻击者使用网络诊断工具（如 traceroute）来进行这项工作，收集到的信息的集合被称为链路图（link map）。攻击者依据链路图筛选目标链路，一般筛选的目标链路流量密度较大，数据传输稳定，是用户访问网络服务的主干链路。攻击者选定目标链路后，将组织大量僵尸主机向目标链路发送低速合法数据流以消耗其带宽，导致链路丢包率和 RTT 值大幅上升，实现对目标链路的阻塞。链路泛洪攻击步骤如图 1 所示。

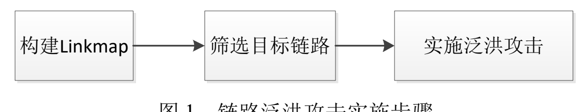


图 1　链路泛洪攻击实施步骤

SDN 网络是一种新型网络架构，其显著特点是数据转发功能与控制功能分离，逻辑集中控制，实现对网络流量的灵活控制。Openflow 作为一种开源协议目前已成为 SDN 的标准，SDN 网络架构分为应用层，控制层与基础设施层，其中控制层是核心，通过 Openflow 信道向基础设施层的交换机下发流表转发规则，可见 Openflow 信道是控制层实现对全网有效控制的基础。Openflow 信道是基于 TCP 的 6633 端口建立的，其可靠性

收稿日期：2017-12-10；**修回日期：**2018-03-04　**基金项目：**国家“863”计划资助项目（2012AA012704）；郑州市科技领军人才资助项目（131PLJRC644）

作者简介：蔡佳晔（1992-），男，云南昆明人，硕士研究生，主要研究方向为网络安全（cjy19920723@126.com）；张红旗（1962-），男，教授，博导，主要研究方向为网络安全、等级保护和信息安全管理；宋佳良（1993-），男，陕西西安人，硕士研究生，主要研究方向为信息安全漏洞管理.

有底层传输协议保证，同样会受到链路泛洪攻击的威胁。一旦攻击者对 Openflow 信道实施链路泛洪攻击，控制层面将无法及时有效地回应来自数据转发层的流表请求，也无法实时掌握全网动态，导致控制层面失去逻辑集中控制功能，达到间接破坏 SDN 网络的目的。因此防范针对 Openflow 信道的链路泛洪攻击具有重要意义。

针对链路泛洪攻击的防御技术，学者们做了如下研究。文献[3]提出 LinkScope 技术，采用端到端逐跳技术捕获异常链路性能下降来检测链路泛洪攻击;文献[4]使用修改后的路由器，可将低速攻击流从合法流量中检测出来，并保护合法流量;文献[5]使用 SDN 流量工程，临时增加目标链路的逻辑带宽，迫使攻击者增加攻击成本，从而使得攻击隐蔽性减弱;文献[6]提出软件定义蜜罐技术，引诱 traceroute 数据包进入蜜网，这样攻击者收集的是通往蜜网的链路，保护真正的网络服务链路不被攻击者探测到;文献[7]提出一种名为 LFADefender 的链路泛洪攻击防御架构，该系统利用 SDN 网络全局视图，流回溯功能以及网络虚拟化的弹性部署特性检测和缓解链路泛洪攻击。

以上研究大部分为攻击发生后采取的检测和缓解措施，在防御态势上处于被动一方。本文借鉴移动目标防御思想（moving target defense,MTD），采取主动防御姿态，提出一种针对 Openflow 信道链路泛洪攻击的防御方法。首先，在 Openflow 交换机北向接口处部署流量监控服务器，每隔固定时间段抓取 Openflow 信道中的数据包，统计 ICMP 超时报文的数量;其次，运用 Renyi 熵分析攻击者在构建 Openflow 信道 Linkmap 过程中产生的 ICMP 超时报文数量变化，以此判断是否出现攻击前兆。最后，一旦出现攻击前兆由流量监控服务器向控制器发出攻击预警，控制器启动交换机-控制器连接迁移机制，将交换机迁移至新的控制器下并使用新的 Openflow 信道与之通信。

1　Traceroute

Traceroute 是 Linux 系统用于路由探测的程序，通过 ICMP“超时”和“端口不可达”两种消息配合记录通向目标主机路径的路由。具体原理如图 2 所示。

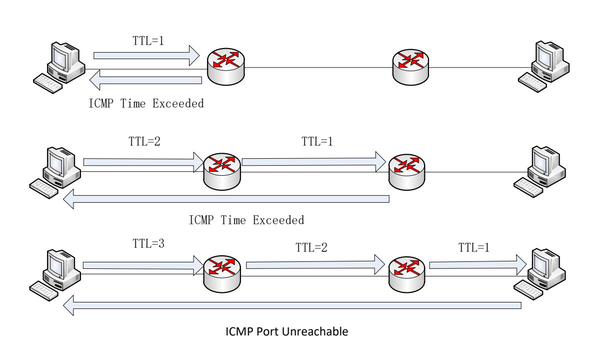
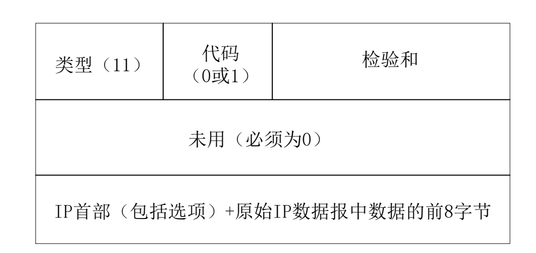


图 2　Traceroute 程序原理

Traceroute 程序利用增加数据包存活时间(TTL)值实现路由探测功能，每当数据包经过一个路由器，TTL 值就会减 1。当 TTL 值减为 0 时，路由器便丢弃数据包并向发送者传递 ICMP Time Exceeded 报文。Traceroute 程序一般首次发送 TTL 值为 1 的 3 个数据包，之后发送 3 个 TTL 值为 2 的数据包，依此类推。当 traceroute 程序收到 ICMP Port Unreachable 消息时，表明发送的数据包已到达目的主机，因为程序发送的数据包目标端口值一般选择应用程序都不会使用的号码(30000 以上)。

综上所述，某个用户使用 traceroute 程序进行路由探测的过程中会产生大量的 ICMP Time Exceeded 消息报文，其报文格式如下



类型（11）	代码（0或1）	检验和
未用（必须为0）		
IP首部（包括选项）+原始IP数据报中数据的前8字节		

图 3　ICMP Time Exceeded 报文格式

ICMP Time Exceeded 报文有两种，本文主机讨论 ICMP 报文是在 TTL 值为 0 时产生的，因此其代码字段为 0。当代码字段为 1 时，为“组装报文超时”的 ICMP 报文。

2　Renyi 熵

信息熵用于刻画随机变量的不确定性，熵值越高，变量随机性越大，熵值越低，变量随机性越小，确定度越高。信息熵在各个领域都有大量应用，如香农熵和 Tsallis 熵，但针对小流量的度量，Renyi 熵相比香农熵更能增大两个分布之间的差异[8]。Renyi 熵定义如下：

$$H_\alpha(x)=\frac{1}{1-\alpha}\log_2\left(\sum_{i=1}^{n}p_i^\alpha\right)\tag{1}$$

满足 $p_i\in\{p_1,p_2\cdots p_n\}$，pi 是随机变量 x_i 的概率分布。$\alpha\ge0,\alpha\ne1$。

当 $\alpha=0$ 时得最大值

$$\max(H_\alpha(x))=\log_2(n)\tag{2}$$

当 $\alpha\to1$ 时，Renyi 熵收敛于香农熵，证明如下：

$$\lim_{\alpha\to1}H_x(\alpha)=\lim_{\alpha\to1}\frac{1}{1-\alpha}\log_2\left(\sum_{i=1}^{n}p_i^\alpha\right)=\lim_{\alpha\to1}\frac{\sum_{i=1}^{n}p_i^\alpha\ln p_i}{\sum_{i=1}^{n}p_i^\alpha\ln2}\tag{3}$$

由于 $\sum_{i=1}^{n}p_i^\alpha=1$，所以有

$$\lim_{\alpha\to1}H_x(\alpha)=-\sum_{i=1}^{n}p_i^\alpha\bullet\log_2p_i\tag{4}$$

当 $\alpha\to0$ 时，有

$$\frac{\partial H_\alpha(x)}{\partial\alpha}\le0\tag{5}$$

表明 $H_\alpha(x)$ 是一个随 α 增大而减小的递减函数。

3 链路泛洪攻击主动防护原理

链路泛洪攻击防护原理如图 4 所示。

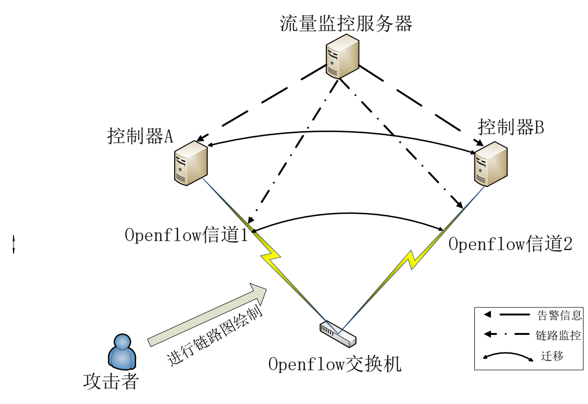


图 4 链路泛洪攻击防护原理

Openflow v1.4.0 版本的协议支持交换机与多个控制器相连以便于两者之间连接关系的调整。因此图中交换机与两个控制器相连，控制器 A 为 master 控制器，用 Openflow 信道 1 与之相连，控制器 B 为 slave 控制器，用 Openflow 信道 2 与之相连。正常情况下交换机主要通过信道 1 与 master 控制器进行通信，当 master 控制器 A 收到链路泛洪预警信息时，启动交换机迁移机制，将控制器 B 变为 master 控制器并使用信道 2 进行通信。由于攻击者并不知道交换机与控制器之间的通信信道发生变化，仍然对信道 1 进行攻击，显然攻击未能达到预期效果，控制器与交换机之间的通信没有受到影响。当攻击者发现攻击无效后，必须再次发送探测数据包进行链路图的绘制工作及定位目标链路，无疑增加攻击者的难度和成本。

攻击者在发动针对 Openflow 信道的 DDoS 攻击前，要进行链路图的收集工作。通常使用 traceroute 程序发送数据包进行路由探测，如前文所述在探测链路的过程中会产生大量的 ICMP Time Exceeded 消息，造成一段时间内 ICMP 包分布发生变化，基于 traceroute 程序这一特性，且 ICMP 包在实际网络中属于小流量行为，本文使用 Renyi 熵来描述 Openflow 信道中 ICMP 包的分布情况。

在流量监控服务器部署抓包程序，每隔固定的时间段监控自网络搭建以来的数据包数量 Mi 作为监控数据，以 ICMP Time Exceeded 报文为统计对象统计其数量 mi 并作为统计数据。将监控数据 Mi，统计数据 mi 以二元数组的形式存储在以时间增序的缓存队列里，如图所示为滑动时间窗口[9]，属于滑动时间窗口内的数据将作为主动防御算法的输入。主动防御算法循环提取缓存队列中的监控数据和统计数据，并计算 Renyi 熵，当判断熵值出现异常后向 master 控制器和 slave 控制器发出链路泛洪预警信息。

本文提出的交换机与控制器的连接关系变化过程如下图 6 所示。假设在迁移过程中控制器 A 不再发送和迁移无关的新信息给交换机处理。

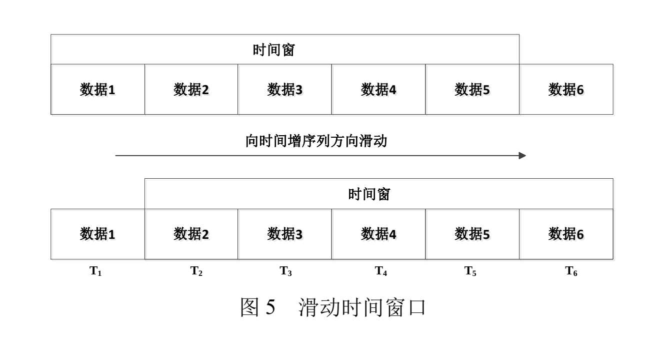


图 5 滑动时间窗口

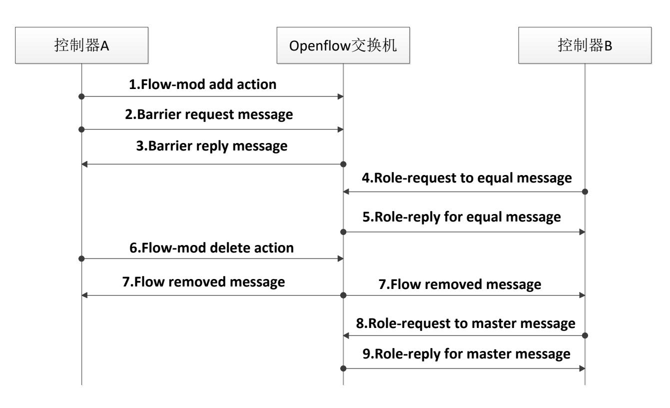


图 6 交换机-控制器连接迁移流程

a）控制器 A 向交换机发送添加流表项的指令，并将一条虚假的流表项添加进交换机中。

b）为了确保交换机安装该虚假流表项，控制器向交换机发送 barrier-request 消息。

c）交换机安装虚假流表项后向控制器发送 barrier-reply 消息回应控制器发送的 barrier-request 消息。

d）控制器 B 向交换机发送 role-request 消息，申请将自己对交换机的身份从 slave 转变为 equal。

e）交换机向控制器 B 发送 role-reply 消息告知其身份转变已完成。能够接收交换机发送的异步消息（asynchronous message），为迁移做好准备。

f）控制器 A 向交换机发送 flow-mod 消息，指示交换机将之前安装的虚假流表项删除。

g）交换机同时向控制器 A 和控制器 B 发送 flow-removed 消息。

h）控制器 B 收到 flow-removed 消息后发送 role-request 消息给交换机请求将自己的角色转变为 master。

i）交换机向控制器 B 发送 role-reply 消息，通知控制器 B 身份转变已完成。同时根据 Openflow 协议，控制器 A 的角色自动设置成 slave。

4 主动防御算法

本文通过研究攻击者使用的链路探测程序 traceroute 的原理，分析运行过程中出现的特征与链路泛洪攻击的关联，提出了一种针对 Openflow 信道链路泛洪攻击的主动防御算法，提高的 SDN 的稳定性和健壮性。图 7 给出算法的流程。

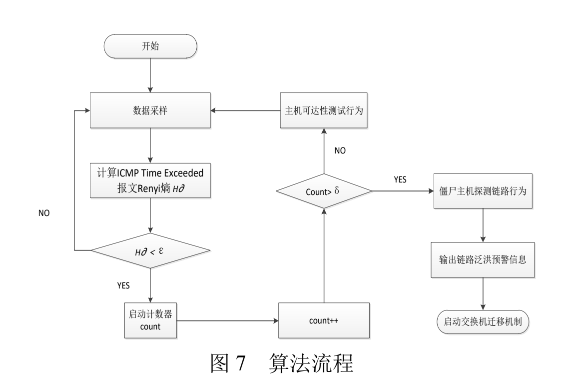


图 7　算法流程

a）循环读取时间窗口内的监控数据和统计数据

b）计算 ICMP Time Exceeded 报文的 Renyi 熵，若熵值高于预警阈值 ε，则返回上一步，若低于预警阈值 ε，则进行下一步。

c）启动计数器 count，其值加 1。

d）判断计数器 count 值是否大于告警阈值 δ，若不大于阈值 δ 则判定为正常主机的链路连通性测试，并返回步骤 a)。若大于阈值 δ，则认定为僵尸主机的链路探测行为，输出链路泛洪预警信息，并进行下一步。

e）启动交换机迁移机制。

在实际 SDN 中部分主机为测试端到端的连通性会发送 ICMP 报文，也同样可能会造成 ICMP Time Exceeded 消息报文数量突变，为了降低算法误报率，避免因交换机频繁迁移导致的网络性能下降，设立一个告警阈值 δ。当 Renyi 熵值低于预警阈值 ε 的次数超过 δ 时，认定为正常主机的链路连通性测试，当次数高于阈值 δ，认定为僵尸主机链路探测行为。阈值 ε 和 δ 需经实验确定。

在算法复杂度方面，设待检测的数据样本总数为 N，算法中两个循环的关系并不是嵌套关系，而是互斥关系，因此可得算法复杂度为 O(N)。

算法：主动防御算法

(1)*do readData*　//循环读取时间窗口内的监控数据和统计数据

(2)　*H∂ = calculate(ICMP)*　*//计算 ICMP Time Exceeded 报文的 Renyi 熵 H∂*

(3)*while H∂< ε*　//若熵值低于预警阈值 ε，重新读取数据

(4) *count++*　//低于预警阈值 ε，count+1

(6)*if*　*count>δ*

(7)　*then alarm()*　*//僵尸主机的链路探测行为，输出预警*

(8)　*then 启动交换机迁移机制*

(9)*else*　*continue*　//正常主机的链路连通性测试

(10) End

5　仿真实验

实验拓扑　本文实验环境基于 Mininet 仿真平台，使用 Openflow v1.4 版本协议，控制器使用 Floodlight 版本，交换机为 Open vSwitch 和刷写了 OpenWRT 开源系统,并能支持 Openflow v1.4 版本的路由器。搭建的网络拓扑如图 8 所示

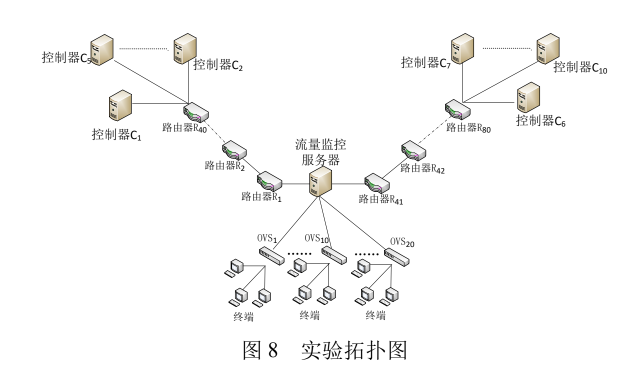


图 8　实验拓扑图

实验拓扑中 Openflow 交换机个数为 20，控制器个数为 10，路由器个数为 80。网络初始状态下控制器 C1 至 C5 为 master 控制器，C6 至 C10 为 slave 控制器。路由器用于模拟真实网络中的 Openflow 信道，其中 R1 至 R40 模拟 Openflow 信道 1，R41 至 R80 模拟 Openflow 信道 2。流量监控服务器部署在 Openflow 交换机北向接口处，每个交换机和 3 台终端相连。

6　实验结果分析

实验首先模拟僵尸主机的不同链路探测强度，将探测强度分为三个等级，一级探测强度模拟僵尸主机使用 traceroute 程序发送 TTL 值依次为 1 至 10 的数据包。二级探测强度模拟僵尸主机使用 traceroute 程序发送 TTL 值依次为 1 至 20 的数据包。三级探测强度模拟僵尸主机使用 traceroute 程序发送 TTL 值依次为 1 至 30 的数据包。用于模拟 Openflow 信道的路由器为 40 台，因此三级强度已接近完成链路探测总量的 75%。图 9~11 为三个探测强度下 ICMP Time Exceeded 报文的 Renyi 熵和香农熵的变化曲线。

在 20 s 时模拟僵尸主机对 Openflow 信道 1 依次实施一、二、三级强度的链路探测，图 9 显示一级探测强度下检测到两次 ICMP time exceeded 报文的熵值偏离正常值的情况并在 27s 处回归正常水平。其中香农熵值偏离程度最小；随着阶数 α 的增大， Renyi 熵值偏离程度逐渐增大，在 α=10 时偏离程度最大，达到 0.206 8。图 10 显示二级探测强度下检测到 4 次熵值偏离正常值的情况并在32s处回归正常情况，阶数 α=10 的 Renyi 熵偏离最大，达到 0.249 0。图 11 显示检测到 8 次熵值偏离情况，阶数 α=10 的 Renyi 熵偏离幅度最大，达到 0.3898，熵值在 40 s 处才回归正常水平。

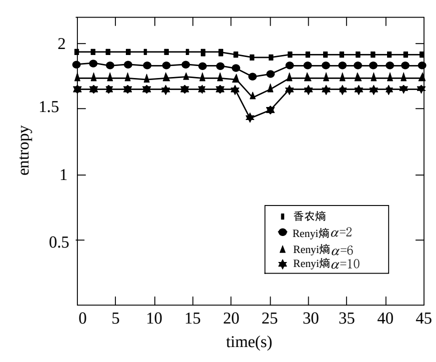


图 9　一级探测强度熵值

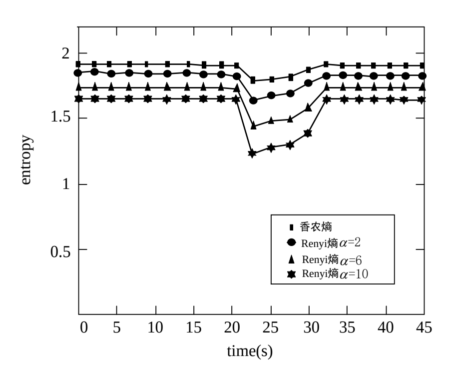


图 10　二级探测强度熵值

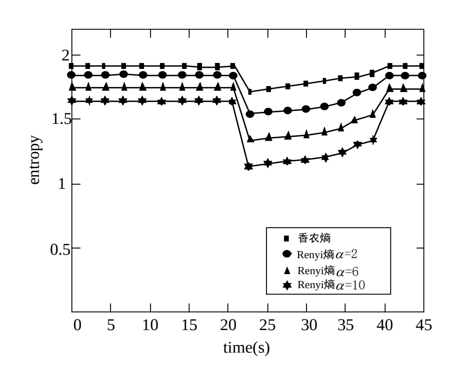


图 11　三级探测强度熵值

综上所述，随着探测强度的增大，熵值偏离的幅度也不断加大，这是因为探测过程中生成的 ICMP Time Exceeded 报文数量占总流量的比重不断升高，但 ICMP 报文在实际网络中是小流量行为，增加比例较小，香农熵变化幅度有限，无法及时对 ICMP 流量的变化作出反映，检测灵敏度较低。而 Renyi 熵无论在哪种探测强度下，都能“放大”流量特征的变化，检测灵敏度高。表 1~3 为不同探测强度下香农熵和 Renyi 熵的具体值。通过对比，Renyi 熵在阶数 α=10 时检测灵敏度最高，正常平均熵值为 1.6439，所以将阈值 ε 设为 1.6439。当检测到熵值偏离 8 次时，攻击者已完成约 75%的探测量，因此本文将阈值 δ 设为 8，避免因小流量变化导致频繁启动交换机迁移，降低整个 SDN 网络的性能。

表 1　一级探测强度各阶数 Renyi 熵

阶数	正常平均熵值	最低熵值	拐点差
香农熵	1.7851	1.7809	0.0042
α=2	1.7384	1.6894	0.0490
α=6	1.6968	1.5921	0.1047
α=10	1.6439	1.4371	0.2068

表 2　二级探测强度各阶数 Renyi 熵

阶数	正常平均熵值	最低熵值	拐点差
香农熵	1.7851	1.7249	0.0602
α=2	1.7384	1.6461	0.0923
α=6	1.6968	1.4846	0.2122
α=10	1.6439	1.3949	0.2490

表 3　三级探测强度各阶数 Renyi 熵

阶数	正常平均熵值	最低熵值	拐点差
香农熵	1.7851	1.7031	0.0820
α=2	1.7384	1.6157	0.1227
α=6	1.6968	1.3629	0.3339
α=10	1.6439	1.2541	0.3898

在确定算法阈值后进行算法防护效果测试，Openflow v1.4 协议中规定当一个 Openflow 交换机与 master 控制器的通信中断时会进入 STANDALONE 状态，进入该状态的 Openflow 交换机会转变成传统二层交换机建立 MAC 表进行数据包转发工作。

实验模拟攻击者对 Openflow 信道 1 发动链路泛洪攻击的全过程。下图描绘了实验过程中处于 STANDALONE 状态的 Openflow 交换机的数量，在 0~30 s 模拟攻击者发送 traceroute 数据包进行链路图收集工作，30 s 时对 Openflow 信道 1 进行模拟链路泛洪攻击，可以看到当没有部署动态防御算法时，随着时间的推移变成 STANDALONE 状态的交换机数量急剧上升，在 40 s 时所有交换机均处于 STANDALONE 状态，此时表明 master 控制器无法与交换机进行通信，SDN 网络彻底瘫痪，Openflow 交换机退化为传统二层交换机。

当部署了动态防御算法后，可以看到仅有 2 台交换机处于 STANDALONE 状态，原因是有的交换机还未完成迁移流程时与 master 控制器通信的链路就被阻断，尤其在交换机处理 barrier 消息时需要将之前控制器发送的消息处理完毕后才能回复 barrier reply 消息，无疑增加了迁移所用的时间，但整体防御效果符合理论预期。

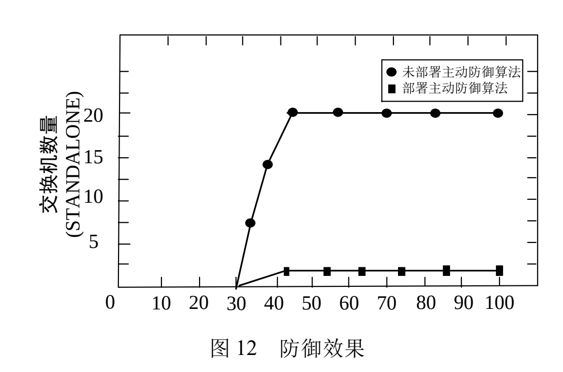


图 12　防御效果

7　结束语

本文提出了一种基于 Renyi 熵的 Openflow 信道链路泛洪攻击主动防御方法，在 Openflow 交换机北向接口部署流量监控服务器，监控 Openflow 信道内 ICMP 超时报文数量，当报文数量出现异常时启动交换机迁移机制，交换机使用新 Openflow 信道与新 master 控制器进行通信。经实验证明主动防御方法能有效避免控制器与交换机之间通信链路受到链路泛洪攻击的影响,确保控制器和交换机能持续交互提供网络服务,增强了 SDN 的健壮性。今后的研究工作将继续围绕 SDN 控制层面的网络

动态防御技术研究，提高 SDN 整体安全性。

参考文献：

[1] Kang M S, Lee S B, Gligor V D. The crossfire attack [C]// Security and Privacy. 2013: 127-141.

[2] Studer A, Perrig A. The coremelt attack [C]// Lecture Notes in Computer Science, vol. 2009: 37-52.

[3] Xue L, Luo X, Chan E W W, *et al.* Towards detecting target link flooding attack [C]// Proc of USENIX Conference on Large Installation System Administration. [S. l.] : USENIX Association, 2014.

[4] Lee S B, Kang M S, Gligor V D. CoDef: collaborative defense against large-scale link-flooding attacks [C]// Proc of ACM Conference on Emerging NETWORKING Experiments and Technologies. New York: ACM Press, 2013: 417-428.

[5] Kang M S, Gligor V D, Sekar V, *et al.* SPIFFY: inducing cost-detectability tradeoffs for persistent link-flooding attacks [C]// Proc of Network and Distributed System Security Symposium. 2016.

[6] Kim J, Shin S. Software-Defined HoneyNet: towards mitigating link flooding attacks [C]// Proc of IEEE//IFIP International Conference on Dependable Systems and Networks Workshop. Washington DC: IEEE Computer Society, 2017: 99-100.

[7] 刘世辉. 基于 SDN 和 NFV 的链路洪泛攻击检测与防御 [D]. 武汉：武汉大学, 2017.

[8] Zyczkowski K. Renyi extrapolation of Shannon entropy [J]. Physics, 2003, 10 (3): 297-310.

[9] 蔡佳晔，张红旗，高坤. 基于 Sibson 距离的 OpenFlow 网络 DDoS 攻击检测方法研究 [J]. 计算机应用研究, 2018, 35 (6) .

[10] 张朝昆，崔勇，唐翯祎，等. 软件定义网络 (SDN) 研究进展 [J]. 软件学报, 2015, 26 (1): 62-81.

[11] Wang Qian, Xiao F, Zhou M, *et al.* Linkbait: active link obfuscation to thwart link-flooding attacks [J]. arXiv: 1703. 09521, 2017.

[12] Wang L, Li Q, Jiang Y, *et al.* Towards mitigating link flooding attack via incremental SDN deployment [C]// Computers and Communication. 2016: 397-402.

[13] 王鹏. 防止链路型 DDoS 攻击的实现方法和系统：中国, CN105049441A [P]. 2015.

[14] 王利明，雷程，马多贺，等. 一种基于转发路径自迁移的链路型 DDoS 防御方法及系统：中国, CN106961387A [P]. 2017.

[15] 陈宇，温欣玲，段哲民，等. 一种大规模 IP 网络多链路拥塞推理算法 [J]. 软件学报, 2017, 28 (7): 1815-1834.